RECEIVED
CENTRAL FAX CENTER
MAY 25 2007

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method, comprising:

generating a first level trusted computing base (TCB) having a plurality of hardware components including a trusted platform module (TPM);

forming an extended TCB by adding a second level TCB to the first level TCB, wherein the second level TCB is software-based; ~~and~~

transferring properties associated with the first level TCB to the second level TCB;

adding one or more levels of software-based TCB to the extended TCB;

transferring the properties associated with the first level TCB to the one or more levels of software-based TCB via one or more levels of TCB interfaces;

storing measured values depending on a level of abstraction of the one or more levels of software TCB; and

using the one or more levels of software TCB independent of hardware-based or software-based implementation of a level of software TCB below the one or more levels of software TCB.

2. (Original) The method of claim 1, wherein the transferring of the properties is performed using a first level TCB interface having at least one of the following operations: secure storage, initiation of software integrity measurement, and attestation.

3. (Original) The method of claim 1, wherein the properties associated with the first level TCB comprise trust and security properties including at least one of the following: tamper-resistant secure storage, tamper-resistant software measurement, tamper-resistant attestation of previously measured values via tamper-resistant signature algorithms, and private keys.

4. (Cancelled)

5. (Original) The method of claim 4, wherein a level of software-based TCB of the one or more levels of software-based TCB of a first system intact with a counterpart level of software TCB of a second system independent of other levels of the one or more levels of software-based TCB of the first system.

6. (Cancelled)

7. (Original) The method of claim 1, wherein the second level TCB is executed independent of the first level TCB using a processor and main memory of a system.

8. (Original) The method of claim 1, wherein the second level TCB and the one or more levels of software-based TCB use encryption keys for attestation and secure storage, the encryption keys are encrypted using protected encryption keys in a TCB level below the second level TCB and the one or more levels of software-based TCB, certified via a signature of the private attestation key of the TCB level below the second level TCB and the one or more levels of software-based TCB, and stored in the TCB level below the second level TCB and the one or more levels of software-based TCB and terminating at the first level TCB being a root of trust for the extended TCB.

9. (Original) A method, comprising:

generating a first level trusted computing base (TCB) having a plurality of hardware components including a trusted platform module (TPM);

forming an extended TCB by adding a second level TCB to the first level TCB, wherein the second level TCB is software-based;

adding a first virtual software TPM to the second level TCB; and

transferring properties associated with a hardware TPM of the first level TCB to the first virtual software TPM.

generate a first virtual container corresponding to the first virtual software TPM, the first virtual container comprises trusted services including at least one of the following: network services, file system services, and provisioning services.

30. (Currently Amended) The machine-readable medium of claim ~~27~~ 24, wherein the sequences of instructions which, when executed by the machine, further cause the machine to:

add one or more virtual software TPMs to the extended TCB, the one or more virtual software TPMs having the properties associated with the hardware TPM of the first level TCB; and

generate one or more virtual containers corresponding to the one or more virtual software TPMs, the one or more virtual containers comprise trusted applications including at least one of the following: login, biometric pattern matching, and protected signal processing.